DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 4 - Internet and E-Mail Privacy

1. References.

   a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

   b. AR 25-2, Information Assurance, 14 November 2003.

   c. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

   d. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

   e. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

   f. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

   g. DoD CIO G & PM No. 4-8460, "GIG Networks," 24 August 2000.

   h. DoD CIO G & PM No. 10-8460, "GIG Network Operations," 24 August 2000.

   i. DoD CIO G & PM No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

   j. 4ID Policy # 5: Passwords.

2. Purpose: The 4ID Internet and electronic mail (E-Mail) system is the primary command and control system for general operational and administrative issues and provides a vehicle for communicating electronically with external resources. It provides a reliable, timely, and direct method of exchanging information, sharing ideas, and eliciting responses.

3. Applicability. This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

   a. Commanders, directors, and supervisors at all levels shall ensure that subordinate personnel are aware of permissible and unauthorized use of the Internet and government E-Mail resources and that inappropriate use may be a basis for disciplinary action.

   b. The 4ID Internet and E-Mail users shall use E-Mail resources responsibly and abide by normal standards of professional and personal conduct at all times.

   c. The Information Assurance Manager (IAM) shall ensure that all IT / IA staff are familiar with the policy and procedures contained herein and that possible criminal activity shall be reported to the IAM immediately for further assessment and appropriate action. Where illegal activity is confirmed, the unit shall be notified by the IAM.

5. Internet and Electronic Mail Privacy Policy and Monitoring of Computer Usage.

a. *NO EXPECTION OF PRIVACY:* The computers and computer accounts given to personnel are to assist them in performance of their jobs. Personnel should not have an expectation of privacy in anything they create, store, send, or receive on the computer system.

b. *NO PRIVACY IN COMMUNICATIONS:* Personnel should never consider electronic communications to be either private or secure. Email may be stored indefinitely on any number of computers, including that of the recipient. Copies of your message may be forwarded to others either electronically or on paper. In addition, email sent to nonexistent or incorrect usernames may be delivered to persons that you never intended.

c. *MONITORING OF COMPUTER USAGE:* The government has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by personnel on the Internet, monitoring chat groups and newsgroups, and reviewing material downloaded from or uploaded to the Internet by users.

d. *BLOCKING INAPPROPRIATE CONTENT.* The government may use software to identify inappropriate Internet sites. Such sites may be blocked from access by government networks. In the event you encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to government blocking software.

e. *PROHIBITED ACTIVITIES:* Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email or other form of electronic communication (bulletin board systems, newsgroups, chat groups), downloaded from the Internet, or displayed on or stored in government computers. Personnel encountering or receiving this kind of material should follow the reporting requirements detailed in paragraph 6 of this policy.

f. *VIRUSES:* Viruses can cause considerable damage to computer systems. Users should never download or accept e-mail attachments from unknown senders or use disks from outside sources without first scanning the material with 4ID -approved virus checking software. If a user suspects that a virus has been introduced into the Government's network, he or she shall notify their Information Assurance Security Officer (IASO), Systems Administrator, or the 4ID Help Desk immediately to obtain advise on the next course of action.

6. Reporting Inappropriate Activity:

a. Users shall submit complaints about inappropriate Internet or E-mail activity to their Information Assurance Manager (IAM), e-mail systems administrator, or Information Assurance Security Officer (IASO).

b. The IAM, IASO and/or systems administrator shall inform a non-compliant user's immediate commander /supervisor, who shall consider disciplinary or other corrective actions, as appropriate. If potential criminal behavior is indicated, the IAM/IASO may be legally obligated to report such activity to the appropriate authorities with the concurrence and involvement of the Information Assurance Manager (IAM).

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding